PROJECT TITLE: Periodic Binomial Coefficients and their Application to Cryptography
and to Solutions of Systems of Polynomial Equations over Finite Fields

Timothy Hodges
Department of Mathematical Sciences
4 French Hall West
Cincinnati, OH 45221-0025
Tel: (513) 556-4040
Fax: (513) 556-3417
Email: timothy.hodges@uc.edu

Project Description

Binomial coefficients occur as the coefficients in the expansion of \((1+x)^n\) as well as in other contexts such as Pascal’s triangle. If one adds every fifth element in a row of Pascal’s triangle one finds a function which is periodic of period 5. Picking an arbitrary row and a general “jump” number one finds a whole family of periodic functions which were shown by Ramus at the end of the nineteenth century to have a surprising trigonometric description. Interestingly, these functions arise naturally in the study of solution of systems of polynomial equations over the finite field with 2 elements. More generally, if one works over a field of order \(q\), the numbers that occur are periodic versions of generalized binomial coefficients. Recent work of Hodges, Schlather and Petit used some properties of these numbers to gain interesting insights into the complexity of Grobner basis algorithms applied to such problems. Many further interesting directions remain open for further study. These include combinatorial study of these functions and their Fourier decomposition, computational experiments which may generate interesting conjectures, and further applications to the problem of understanding systems of polynomial equations over finite fields.

Students undertaking this project should ideally have taken a basic course in abstract algebra or number theory and have experience with Mathematica or basic computer programming.